This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of securing ~~security~~ stored data ~~stored~~ on a computer system, comprising:

providing one of several different password data ~~keys~~ to the computer system;

transforming ~~the security~~ key data with ~~the~~ one of the several different password data ~~key~~ in a reversible fashion to produce encoded ~~secure~~ key data such that the one of the several different password data ~~key~~ is required in order to perform a reverse transform and extract the ~~security~~ key data from the encoded ~~secure~~ key data; and [[,]]

storing the encoded ~~secure~~ key data ~~in a fashion such that a user authorization process is used to retrieve the encoded secure data~~ such that the one of the several different password data ~~key~~ and ~~the~~ one of a plurality of user authorization processes, in combination, provide access to the ~~security~~ key data ~~and such that the stored data within the computer system is encoded~~,

wherein ~~a same security~~ the key data is encoded with each of said several different password data ~~keys~~ to provide different encoded ~~secure~~ key data for each user authorization process such that a combination of ~~user authorization using~~ one of said user authorization processes and ~~any of said several different~~ a respective password data ~~keys~~ of the several different password data allows for retrieval and decoding of the ~~same security~~ key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

2. (Canceled).

3. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 1, wherein each encoded ~~secure~~ key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different password data ~~keys~~ allows for retrieval and decoding.

4. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 1, wherein the user authorization process is a biometric information verification process.

5. (Canceled)

6. (Currently Amended) A method of securing ~~security~~ stored data ~~stored~~ on a computer system, comprising:

providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source and, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

providing one of several different password data ~~keys~~ associated with the first individual identity, the one of the several different password data ~~key~~ being other than stored on the computer system; and

retrieving encoded ~~security~~ key data associated with the biometric information, and using the one of the several different password data ~~key~~ for decoding the encoded ~~security~~ key data,

wherein ~~a same security~~ the key data is encoded with said several different password data ~~keys~~ to provide different encoded ~~secure~~ key data for each user authorization process such that a combination of user authorization by said biometric information source in one of said user authorization processes and ~~any of said several~~ a different of the several different password data ~~keys~~ allows for retrieval and decoding of the same security data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

7. (Canceled) ~~A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system~~.

8. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 6, wherein the decoded ~~security~~ key data is for allowing access of the stored data to the identified individual.

9. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 6, wherein ~~the step of~~ providing the biometric information source comprises imaging the biometric information source using a contact imager.

10. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 9, wherein the contact imager is a fingerprint imager.

11. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 6, wherein ~~the step of~~ providing the one of the several different password data ~~key~~ comprises ~~the step of~~ providing a password.

12. (Currently Amended) ~~A~~ The method of ~~securing security data stored on a computer system according to~~ claim 6, wherein ~~the step of~~ providing the one of the several different password data ~~key~~ comprises ~~the step of~~ providing information stored on a smart card.

13. (Currently Amended) A method of securing data, comprising:

providing a first information sample to a computer system;

encoding one of several different password data ~~keys~~ in dependence upon the first information sample to produce ~~first security~~ key data, the key data for use in decoding stored encoded data;

providing at least one biometric information sample; and

securing the ~~first security~~ key data in dependence upon ~~at least one of~~ the at least one biometric information sample,

wherein ~~a same security~~ the key data is encoded with said several different password data ~~keys~~ to provide different encoded ~~secure~~ key data for each user authorization process

such that a combination of user authorization using said biometric information sample in one of said user authorization processes and ~~any of said several~~ a different one of the several different password data ~~keys~~ allows for retrieval and decoding of the ~~same security~~ key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

14. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 13, wherein ~~the step of~~ providing a first information sample to a computer system comprises hashing the first information sample to produce a first hash value.

15. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 13, comprising:

providing a second other information sample to the computer system;

hashing the second information sample to produce a second hash value;

encoding the ~~key~~ one of the several different password data in dependence upon the second hash value to produce second ~~security~~ key data; and

securing the second ~~security~~ key data in dependence upon ~~at least one of~~ the at least one biometric information sample.

16. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 13, wherein ~~the step of~~ providing the first information sample to a computer system comprises ~~the step of~~ providing a password.

17. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 13, wherein ~~the step of~~ providing the first information sample to a computer system comprises ~~the step of~~ providing information stored on a smart card.

18. (Canceled)

19. (Currently Amended) A method of securing data comprising:

providing a first information sample to a computer system;

providing at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding one of several different password data ~~keys~~ in dependence upon the encoded biometric sample to produce ~~first security~~ key data~~, the key data for use in decoding stored encoded data~~; and

securing the ~~first security~~ key data in dependence upon ~~at least one of~~ the at least one biometric information sample,

wherein the ~~first security~~ key data is encoded with said several different password data ~~keys~~ to provide different encoded ~~secure~~ key data for each user authorization process such that a combination of user authorization using said biometric information sample in one of said user authorization processes and ~~any of said several~~ a different one of the several different password data ~~keys~~ allows for retrieval and decoding of the ~~first security~~ key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

20. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 19, comprising:

providing a first information sample to a computer system for decoding the encoded biometric sample; and

comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. (Currently Amended) ~~A~~ The method of ~~securing data according to~~ claim 19, wherein ~~the step of~~ providing a first information sample to a computer system comprises hashing the first information sample to produce a first hash value.

22. (Currently Amended) A computer system that secures ~~security~~ stored data ~~stored therein~~, comprising:

an input device that provides at least one of several different password data ~~keys~~ to the computer system;

a processing device that encodes ~~a same security~~ key data with said several different password data ~~keys~~ in a reversible fashion to produce different encoded ~~secure~~ key data for each user authorization process such that respective ones of the several different password data ~~keys~~ are required in order to perform a reverse transform and extract the ~~security~~ key data from the encoded ~~secure~~ key data, wherein the processing device uses the key data for performing at least one of encrypting and decrypting the stored data on the computer system;

a memory device that stores the encoded ~~secure~~ key data; and

a user authorization process that retrieves the encoded ~~secure~~ key data from the memory device such that at least one of the several different password data ~~keys~~ and the user authorization process, in combination, provide access to the ~~security~~ key data, wherein a combination of user authorization using said user authorization process and ~~any of said several~~ a different one of the several different password data ~~keys~~ allows for retrieval and decoding of the ~~same security~~ key data.

23. (Currently Amended) ~~A~~ The computer system according to claim 22, further comprising a plurality of user authorization processes, wherein each encoded ~~secure~~ key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different password data ~~keys~~ allows for retrieval and decoding of the ~~security~~ key data.

24. (Currently Amended) ~~A~~ The computer system according to claim 22, wherein the user authorization process is a biometric information verification process.

25. (Currently Amended) ~~A~~ The computer system according to claim 22, wherein the one of the several different password data ~~keys~~ includes a password.

26. (Currently Amended) A computer system that secures ~~security~~ stored data ~~stored therein~~, comprising:

means for comparing a biometric information source against stored templates associated with the biometric information source and, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

an input device that provides to the computer system a different password data ~~key~~ for each user authorization process associated with the first individual identity, the password data ~~key~~ being other than stored on the computer system; ~~and~~

means for retrieving encoded ~~security~~ key data associated with the biometric information and for using the password data ~~key~~ for decoding the encoded ~~security~~ key data, wherein a combination of user authorization by said biometric information source in one of said user authorization processes and ~~any of said several~~ a different one of the different password data ~~keys~~ allows for retrieval and decoding of the same ~~security~~ key data; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

27. (Canceled) ~~A computer system according to claim 26, further comprising means for performing at least one of encrypting and decrypting data on the computer system using the decoded security data.~~

28. (Currently Amended) ~~A~~ The computer system according to claim 26, wherein the decoded ~~security~~ key data allows access to the stored data by the identified individual.

29. (Currently Amended) ~~A~~ The computer system according to claim 26, wherein the comparing means comprises a contact imager that images the biometric information source.

30. (Currently Amended) ~~A~~ The computer system according to claim 29, wherein the contact imager is a fingerprint imager.

31. (Currently Amended) ~~A~~ The computer system according to claim 26, wherein at least one of said ~~several~~ different password data ~~keys~~ comprises a password.

32. (Currently Amended) ~~A~~ The computer system according to claim 26, wherein at least one of said different password data ~~keys~~ is stored on a smart card.

33. (Currently Amended) A computer system that secures stored data ~~stored therein~~, comprising:

an input device that provides a first information sample to the computer system;

means for encoding a ~~same security~~ key data with different password data ~~keys~~ for each user authentication process in dependence upon the first information sample to produce first security data, the key data for use in decoding the stored ~~encoded~~ data;

a biometric input device that provides at least one biometric information sample; ~~and~~

means for securing the first security data in dependence upon at least one of the at least one biometric information sample in one of said user authorization processes, wherein a combination of user authorization using said biometric information sample and any of said ~~several~~ different password ~~data~~ keys allows for retrieval and decoding of the ~~same security~~ key data; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

34. (Currently Amended) ~~A~~ The computer system according to claim 33, further comprising means for hashing the first information sample to produce a first hash value.

35. (Currently Amended) ~~A~~ The computer system according to claim 33, wherein the first information sample comprises a password.

36. (Currently Amended) ~~A~~ The computer system according to claim 33, wherein the first information sample is stored on a smart card.

37. (Currently Amended) ~~A~~ The computer system according to claim 33, wherein the encoding means encrypts data using the key data.

38. (Currently Amended) A computer system that secures stored data ~~stored therein~~, comprising:

an input device that provides a first information sample to the computer system;

a biometric input device that provides at least one biometric information sample to the computer system;

means for encoding the at least one biometric information sample using the first information sample and for encoding one of several different password data ~~keys~~ in dependence upon the encoded biometric sample to produce ~~first security~~ key data, the key data for use in decoding stored encoded data, wherein the ~~first security~~ key data is encoded with said different password data ~~keys~~ for each user authorization process to provide ~~several~~ different encoded ~~secure~~ key data such that a combination of user authorization using said biometric information sample in one of said user authorization processes and any of said ~~several~~ different password data ~~keys~~ allows for retrieval and decoding of the ~~first security~~ key data; ~~and~~

means for securing the ~~first security~~ key data in dependence upon at least one of the at least one biometric information sample; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

39. (Currently Amended) ~~A~~ The computer system according to claim 38, comprising:

means for decoding the encoded biometric sample using a first information sample provided by the input device; and

means for comparing the decoded biometric sample against stored templates associated with the biometric information source.

40. (New) A computer readable storage medium for securing stored data on a computer system, the computer readable storage medium having computer executable instructions stored thereon that when executed perform the method, comprising:

providing one of several different password data to the computer system;

transforming key data with one of the several different password data in a reversible fashion to produce encoded key data such that the one of the several different password data is required in order to perform a reverse transform and extract the key data from the encoded key data; and

storing the encoded key data such that the one of the several different password data and one of a plurality of user authorization processes, in combination, provide access to the key data,

wherein the key data is encoded with each of said several different password data to provide different encoded key data for each user authorization process such that a combination of one of said user authorization processes and a respective password data of the several different password data allows for retrieval and decoding of the key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

41. (New) The computer readable medium of claim 40, wherein each encoded key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different password data allows for retrieval and decoding.

42. (New) The computer readable medium of claim 40, wherein the user authorization process is a biometric information verification process.